

# Information Leak Prevention: Tackling The Insider Threat

By Ariel Peled

While hackers still pose a significant threat that requires organizational perimeters to be fortified, purely protecting the perimeter is not sufficient. Risks from the inside are increasingly getting management- and board-level attention due to their high profile and costly nature. External threats are typically mitigated by software and hardware tools that lock outside access to corporate resources through network firewalls, identity management solutions and intrusion prevention systems. Using similar types of controls inside corporate networks is not feasible because they can be disruptive to everyday workflows and can considerably reduce employee productivity.

## Two Elements of Information Control

In order to secure organizational resources within the perimeter while preserving employee productivity, a different set of controls must be used to protect an organization's information, applications and infrastructure. While applications and infrastructure can be secured through access control systems, sensitive (both confidential and private) information is still at a high risk. Information security entails control of two elements: information at rest and information in transit.

Information at rest can be stored in either encrypted or non-encrypted format and protected via access control lists on file systems, applications, and databases. Physical and logical data location and access controls associated with sensitive data should be designed when an IT project is planned.

Information in transit entails yet another set of requirements. First, sensitive data must be accurately defined to allow for proper controls. Secondly, because of the variety of business communication channels available, multiple channels and protocols must be monitored to ensure that the information is being sent to the proper, authorized recipients. And finally, internal policies must be maintained to determine whether and how different types of sensitive data may be distributed to various recipients and groups.

## Shortcomings of Existing Control Schemes

One of the inevitable problems of the fast pace of today's business world is that business processes change too quickly for IT systems and procedures to follow. In many cases, controls that were designed to enforce certain business processes become obsolete when those processes change. In fact, these controls may not enforce and audit the newly formed business process, and they sometimes tend to hamper it.

Just as water seeks the easiest path to continue its flow, employees tend to find paths of least resistance in the business world. In order to expedite

workflows, workers will invariably find ways to bypass obtrusive and obsolete controls, reducing the effectiveness of these controls altogether.

## How E-mail Changed the Risk Landscape

So, how do employees bypass current security measures? The simplest way that trusted insiders circumvent existing security measures is through e-mail. As the number one business tool today, e-mail is used by virtually every kind of organization by the vast majority of employees. In addition, with little or no controls over attachments and message content, it is extremely easy for any employee, temporary worker, or consultant to send confidential or private information to anyone else with an e-mail address with a few clicks of a mouse. Moreover, many organizations use e-mail as the fallback file transport vehicle for proprietary information. This practice clearly highlights an inadequately controlled business process.

While e-mail allows employees to compensate for an outdated controls schema, it creates a considerable risk (exposure to liability, regulatory oversight, and embarrassing incidents) as business processes are now much less controlled and audited. While the evolved business processes now have weaker controls over the integrity and consistency of their information products, the controls over the disclosure of the information used by and produced by these processes are slim to none.

Information distributed via e-mail rarely follows the information classification and access control processes implemented by the organization. Employees are often unaware of their own mistakes, and do not realize they may be distributing sensitive information to unauthorized parties—an information leak. These mistakes and misconceptions require a reasonably implemented approach towards identifying and preventing such violations of internal policies. Automating the detection of these incidents can provide more consistent adherence to corporate policies by supporting existing business processes in a controlled fashion.

## Increasing Stakes of Information Leakage

While information leakage is a serious risk, the problem is not new by any means. Information technology auditors have been warning executive management for years about these issues, but have not received the proper attention until only recently. These information breaches are taking center stage now for two reasons: frequency and visibility. Leaks are occurring more frequently as the volume of business communication has increased, particularly via e-mail, web mail, instant messaging, faxing,

and more. Also, the media is focusing more and more on information leak events, as those gain increasing public attention.

One notable event, before Sarbanes-Oxley was enacted, involved Disney Chairman and CEO Michael Eisner erroneously e-mailed quarterly financial results to an ABCNews employee instead of a Disney employee because they had similar names. Luckily, the ABCNews employee reported the error to Eisner, thereby averting the repercussions of a suspected insider trading scandal. Since that incident, Eisner has been quoted saying, "If anything will bring about the downfall of a company... it is blind copies of e-mails that should never have been sent in the first place." In the aftermath of Enron, the Sarbanes-Oxley act specifically required public companies to tighten their entire control scheme over any business processes touching financial results, and just as importantly, holds executives responsible for any discrepancies.

Increasing media attention around information leaks has affected the share prices, public perception, and business practices of prominent firms. This high-profile visibility has spurred management to take information leak prevention much more seriously. Additionally, regulatory mandates governing consumer privacy and corporate accountability have also enhanced the degree of attention garnered by the problem of information leakage.

While private financial, customer, and employee information has always been regulated, new standards are helping to define what reasonable steps companies need to take to stay in compliance. These regulations range from registration of publicly traded companies' quarterly results with the SEC to the notification of affected customers in the event of a breach of private information, whether malicious or unintentional, according to California SB1386 (now Civil Code 1798). Similarly, HIPAA and GLBA are driving organizations to protect patient and medical data as well as customer and financial information against unauthorized distribution.

### **Accidents, Mistakes and Broken Business Processes**

These information leaks are not isolated to particular industries and occur with surprising frequency. These incidents carry some undesirable results, so it is imperative to note instances where this can occur. A few recurring scenarios where confidential information is often leaked include:

- ▲ Misdirecting a message to the wrong e-mail address
- ▲ Attaching the wrong document or file
- ▲ Sending a group of zipped documents without thoroughly verifying the contents

Companies that ignore these scenarios open themselves up to unnecessary and costly risks.

In addition to these accidents or mistakes, poorly designed or poorly implemented business processes often emerge when controls are not updated or the business environment has changed. Unfortunately, these broken processes are often discovered only when a painful event occurs. These events occur in a variety of areas including:

- ▲ Customer service
- ▲ Human resources
- ▲ Financial reporting

### **Customer Service**

Many organizations allow customer service representatives to send private customer information to outside recipients with no encryption and no error control mechanisms. These recipients may be customers requesting account information, authorized business partners, or even the home Web mail accounts of representatives trying to finish work at home. These cases compromise the privacy of customer information by creating unprotected islands of data storage.

### **Human Resources**

HR personnel communicate with benefits service providers in order to update existing employees' packages, new employees and employees who have left. Those communications may include private employee information, sometimes in the subject line, and in many cases HR people are not aware of the risk of misdirected e-mails or faxes, and risks of e-mails which are sent in clear text.

### **Financial Reporting**

Another example of information leaks would be the communication of quarterly results. In order to create the final financial report that would go to the SEC, the financial information is extracted from the financial applications and in many cases aggregated into Excel sheets. Those Excel sheets drafts are distributed among the CEO, CFO, CPA firm, senior executives, board members and other employees that help in the process. This is done in several iterations until the final report is produced. Too often, those communications do not have controls in place to reveal history of that report, both in terms of who sent it, who saw it and when, and what where the changes that every participant made.

### **Understanding the Spectrum of Motivations**

Understanding the motivation behind these incidents is key to comprehending how to address the root causes of certain types of leaks. Leaks tend to fall into a variety of tiers based on their underlying motivation: lack of appropriate business tools, lack of policy awareness, accidents, negligence, intentional misuse, malice, and financial gain. As outlined earlier, accidents and unwitting negligence can happen in a variety of scenarios. Unfortunately, an uncontrolled environment also opens the door to intentional misuse, "semi-malicious" acts by employees, fraud and more.

One example of intentional misuse is the sharing of highly confidential mergers and acquisitions (M&A) information prior to deal execution. An employee may share this M&A information with external peers to demonstrate position and contacts as a key insider. Another incident involved accounting interns forwarding a banking organization's trial balance and profit and loss statements to home Web mail accounts. These employees were working towards certified public accountant (CPA) degrees and wanted to study with real life data, but had no intent to distribute it for any monetary gain. Lastly, "blogs" or Web logs have become an addictive recreation for some employees and recently, a Google employee was cited and fired for posting sensitive information about compensation on his personal blog.

"Semi-malicious" acts are not necessarily aimed at harming the organization, but may allow the employee to benefit personally at the organization's expense. For instance, some home loan officers have been cited for forwarding mortgage applications without a client's consent to other lenders with less stringent approval requirements in exchange for finder's fees. These mortgage applications are ripe for identity theft because they

include customers' name and address, social security number, mother's maiden name, credit rating and financial history, and because they can easily be forwarded again once packages have left the originating organization. In many of these cases, the culprits have been motivated by easy money without perceived harm to the organization, but this behavior creates a huge liability for banks and credit unions.

Unfortunately, successful semi-malicious acts may give employees the false perception that corporate assets are fair game to exploit, and may lead to fully malicious or even criminal behavior. This criminal behavior often arises when controls are thought to be absent and financial incentives are substantial. Two notable cases below highlight abuses of private information by insiders motivated by personal economic gains.

In the first event, former America Online (AOL) engineer Jason Smathers tried to smuggle about 92 million customer e-mail addresses in order to sell them to a spammer for \$100,000. The former employee allegedly used another AOL employee's access code to steal AOL's entire database of screen names in May 2003 and sold the stolen information about all 30 million AOL subscribers to a co-conspirator. Luckily, before the deal was consummated, the conspirators were caught.

In the second case, Richard W. Gibson, an employee of the Seattle Cancer Care Alliance at the time, obtained the name, date of birth and social security of a patient by accessing the organization's information systems in October 2003. Gibson knew that the patient was undergoing treatment for a rare and often fatal form of cancer. Using the patient's private information, he managed to obtain several credit cards and used them to buy various items including apparel, jewelry, video games, as well as groceries and gasoline. Gibson was the first person criminally convicted for violating Health Insurance Portability and Accountability Act (HIPAA).

## Risk Mitigation and Corrective Measures

Given the wide variety of motivations and the ingenious ways in which sensitive information can leak out, where can an organization begin to address such an important issue? First and foremost, each organization must assess the gap between its stated policies for handling confidential and private information and actual behavior and practice. A thorough risk assessment will also allow you to identify the greatest vulnerabilities (e.g. content type, departments, individual offenders, employee training, etc.) and focus on faulty business processes. A good risk assessment should also determine what types of information would be most damaging in the event of a leak: (i.e. private customer data, company financials, human resources information, product schematics, or board memos). If this is the first time a gap analysis is being performed, expect radical findings.

Second, based on the gap analysis findings and the related risks, top management must decide on the following:

- ▲ Which risks to accept—what types of risks can management live with, accepting the consequences if and when they materialize. In this case, the policies violated should be adjusted to authorize the actual behavior found in the risk analysis.
- ▲ Which risks to transfer—what types of risks are not tolerable, but are transferable to another entity at an acceptable price. In this case, the policies violated should be adjusted to authorize the actual behavior by outsourcing certain risky business functions or by purchasing appropriate insurance.
- ▲ Which risks to mitigate—what types of risks are not acceptable

without managing their processes. In this case, controls must be put in line of the business communication infrastructure with ability to detect, prevent, and if possible, to correct. Policy enforcement must be automated to provide consistency and measurability of business processes where risk must be managed (e.g. encrypting e-mail transmissions containing private customer information to an authorized recipient).

## Detection, Prevention and Automation


Both detection and prevention of information leaks are required as many regulations compel organizations to act if they have knowledge about a problem. It is necessary to embed any systematic controls in the business communication infrastructure to provide maximum coverage and visibility without interruption to normal workflows. While e-mail is a primary vehicle for information leaks, a good controls scheme should also include Web traffic, internal mail, printers, faxes (both fax servers and legacy faxes) and instant messaging.

Automatic policy enforcement is necessary to provide a wide range of corrective measures when violations are detected. For instance, many healthcare organizations are required to encrypt private patient information but cannot do so with consistency because they often rely on individual care providers to initiate the encryption. This policy enforcement should be triggered without reliance on employee training and without the need for workflow changes. Because of the real-time nature and the volume of business communications today, an automated system is the only feasible approach to apply appropriate corrective measures.

By centrally managing business communication infrastructure controls and information usage policies, a clear and encompassing view of information distribution risks and business process malfunctions can emerge.

## Conclusion

The insider threat is becoming a pressing concern for many organizations as existing controls have grown obsolete and insufficient. Closing the gap between corporate policies and employee behavior requires much more attention to communicating policies and training employees on what the policies mean relative to their specific job functions and tighter control over areas that have rarely been monitored before.

Information Leak Prevention (ILP) is a holistic approach to addressing the issues of privacy, confidentiality, and accountability and requires a 360-degree examination of practice, procedures and systems. An effective ILP effort is best achieved by investing in a staged review and implementation targeting the points of highest priority. The most effective ILP projects start with the most common business communication tools and the information at the highest risk, and evolve over time to address next-level areas of concern. If ILP is a key business goal, information transmission over various communication channels must be supervised in an accurate way and policy breaches must be handled in a non-disruptive fashion. 

---

*Ariel Peled, CIPP, is co-founder and CTO, Vidius Inc.*

<sup>1</sup> The Enterprise Strategy Group (ESG) reports that as much as 75 percent of most companies' intellectual property is contained in the messages and attachments they send through their e-mail systems.